

Claims

What is claimed is:

- 1 1. A method for allocating a resource, comprising the steps of:
 - 2 (a) receiving a resource allocation request from a client;
 - 3 (b) imposing on said client a computational task and a time limit for correct
 - 4 completion of said computational task;
 - 5 (c) receiving verification that said client has correctly performed said
 - 6 computational task within said time limit; and
 - 7 (d) allocating said resource for said client if the verification is received.
- 1 2. The method of claim 1 wherein said resource allocation request comprises a
- 2 network connection request.
- 1 3. The method of claim 1 wherein said step (b) comprises communicating a puzzle
- 2 as at least a portion of said communication task.
- 1 4. The method of claim 3 wherein said step (b) comprises communicating the output
- 2 of a one-way function to said client.
- 1 5. The method of claim 3 wherein said step (b) comprises communicating the output
- 2 of a block cipher to said client.
- 1 6. The method of claim 3 wherein said step (b) comprises communicating the output
- 2 of a function, wherein the input of said function is generated, based at least in part
- 3 on a server secret unknown to said client, and not revealed through correct
- 4 performance of said computational task.

- 1 7. The method of claim 3 wherein said step (b) comprises communicating the output
2 of a function, wherein the input of said function comprises a timestamp and
3 information authenticating the timestamp.

- 1 8. The method of claim 3 wherein said step (b) comprises communicating a puzzle
2 constructed in a self authenticating fashion.

- 1 9. The method of claim 3 wherein said step (b) comprises communicating a hash
2 image and a partially revealed pre-image to said client.

- 1 10. The method of claim 9 wherein said step (c) comprises receiving the remaining
2 pre-image.

- 1 11. The method of claim 3 wherein said step (b) comprises communicating a plurality
2 of sub-puzzles to a client.

- 1 12. The method of claim 11 wherein said step (b) comprises communicating a
2 plurality of independently constructed sub-puzzles.

- 1 13. The method of claim 11 wherein said step (b) comprises communicating a
2 plurality of sub-puzzles wherein each sub-puzzle is constructed with some
3 intended overlap.

- 1 14. The method of claim 1 wherein said step (a) comprises receiving a TCP SYN
2 request.

- 1 15. The method of claim 1 wherein said step (a) comprises receiving a request to open
2 an SSL connection.

- 1 16. The method of claim 1 wherein said step (b) comprises the steps of:

2 (ba) determining if a computational task is to be imposed upon said client
3 based upon the operating circumstances at the time of receiving said
4 resource allocation request from said client; and
5 (bb) if a computational task is determined to be imposed upon said client then
6 selecting a computational task responsive to at least one characteristic of
7 said operating circumstances at the time of receiving said resource
8 allocation request; and
9 (bc) if a computational task is determined to be imposed upon said client then
10 imposing the selected computational task on said client.

1 17. The method of claim 1, wherein said step (a) comprises receiving a resource
2 allocation request comprising a query, or accompanied or preceded by a query
3 concerning whether a server is currently imposing computational tasks.

1 18. A method for procuring a resource comprising the steps of:

- (a) communicating a resource allocation request to a server;
- (b) receiving a computational task from said server;
- (c) performing or delegating the performance of said computational task correctly within a known time limit; and
- (d) communicating to said server a verification that said computational task has been performed correctly within the known time limit.

1 19. The method of claim 18 wherein said resource allocation request comprises a
2 network connection request.

1 20. The method of claim 18 wherein said step (b) comprises receiving said
2 computational task and a time limit for performance of said computational task
3 from said server.

1 21. The method of claim 18 wherein said step (c) comprises solving a puzzle.

1 22. The method of claim 21 wherein said step (c) comprises a linear search of the
2 solution space associated with said computational task.

1 23. The method of claim 18 wherein said step (c) comprises solving a plurality of
2 sub-puzzles.

1 24. The method of claim 18 wherein said step (a) comprises transmitting a TCP SYN
2 request.

1 25. The method of claim 18 wherein said step (a) comprises transmitting a request to
2 open an SSL connection.

1 26. The method of claim 18 wherein said step (a) comprises transmitting a resource
2 allocation request comprising a query, or accompanied or preceded by a query
3 concerning whether a server is currently imposing computational tasks.

1 27. A apparatus for allocating a resource comprising:
2 a first receiver receiving a resource allocation request from a client;
3 a computational task generator for imposing a computational task upon said client
4 for correct performance within a time limit; and
5 a transmitter communicating said computational task to said client;
6 a second receiver receiving a verification from said client that said
7 computational task was correctly performed with said time limit; and
8 an allocator allocating said resource for said client.

1 28. The apparatus of claim 27 wherein said first receiver and said second receiver
2 comprise the same receiver.

1 29. The apparatus of claim 27 wherein said first receiver receives a resource
2 allocation request comprising a network connection request.

1 30. The apparatus of claim 27 wherein said transmitter communicates said
2 computational task and a time limit for performance of said computational task to
3 said client;

1 31. The apparatus of claim 27 wherein said computational task comprises a puzzle.

1 32. The apparatus of claim 31 wherein said puzzle comprises the output of a one-way
2 function.

1 33. The apparatus of claim 31 wherein said puzzle comprises the output of a block
2 cipher.

1 34. The apparatus of claim 31 wherein said puzzle comprises the output of a function,
2 wherein the input of said function is based at least in part on a server secret
3 unknown to said client and not revealed through correct performance of said
4 computational task.

1 35. The apparatus of claim 31 wherein said puzzle comprises the output of a function,
2 wherein the input of said function comprises a timestamp and information
3 authenticating the timestamp.

1 36. The apparatus of claim 31 wherein said puzzle is constructed in a self
2 authenticating fashion.

1 37. The apparatus of claim 31 wherein said puzzle comprises a hash image, and a
2 partially revealed pre-image.

1 38. The apparatus of claim 37 wherein said verification comprises verifying the
2 remaining unrevealed pre-image.

- 1 39. The apparatus of claim 31 wherein said puzzle comprises a plurality of sub-
2 puzzles.
- 1 40. The apparatus of claim 39 wherein said plurality of sub-puzzles are constructed
2 independently.
- 1 41. The apparatus of claim 39 wherein said plurality of sub-puzzles are constructed
2 with some intended overlap.
- 1 42. The apparatus of claim 27 wherein said resource allocation request comprises a
2 TCP SYN request.
- 1 43. The apparatus of claim 27 wherein said resource allocation request comprises a
2 request to open an SSL connection.
- 1 44. The apparatus of claim 27 wherein said computational task is selected responsive
2 to at least one characteristic of the operating circumstances at the time of
3 receiving said resource allocation request.
- 1 45. The apparatus of claim 27 wherein said resource allocation request comprises a
2 query, or is accompanied or preceded by a query concerning whether a server is
3 currently imposing computational tasks.
- 1 46. The apparatus of claim 27 comprising a time limit generator generating a
2 time limit within which said client must correctly perform said
3 computational task;
- 1 47. A apparatus for procuring a resource comprising:
2 a first transmitter communicating a resource allocation request to a server;
3 a first receiver receiving a computational task from said server;

4 a computational task solver correctly performing said computational task
5 within a known time limit; and
6 a second transmitter communicating to said server a verification that
7 said computational task has been performed.

1 48. The apparatus of claim 47 wherein said first transmitter and said second
2 transmitter comprise the same transmitter.

1 49. The method of claim 47 wherein said first transmitter sends a resource allocation
2 request comprising a network connection request.

1 50. The apparatus of claim 47 further comprising a second receiver receiving a time
2 limit for performing said computational task.

1 51. The apparatus of claim 50 wherein said first receiver and said second receiver
2 comprise the same receiver.

1 52. The apparatus of claim 47 wherein said computational task comprises a puzzle.

1 53. The apparatus of claim 47 wherein said computational task performs a linear
2 search of potentially the entire solution space associated with said computational
3 task.

1 54. The apparatus of claim 47 wherein said computational task comprises a plurality
2 of sub-puzzles

1 55. The apparatus of claim 54 wherein said sub-puzzles are constructed
2 independently.

1 56. The apparatus of claim 54 wherein said sub-puzzles are constructed with some
2 intended overlap.

1 57. The apparatus of claim 47 wherein said resource allocation request comprises a
2 TCP SYN request.

1 58. The apparatus of claim 47 wherein said resource allocation request comprises a
2 request to open an SSL connection.

1 59. The apparatus of claim 47 wherein said resource allocation request comprises a
2 query, or is accompanied or preceded by a query concerning whether said server
3 is currently imposing computational tasks.